NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DIVISON: NC DHHS Privacy and Security Office	**POLICY NAME:** Workforce Sanction Violation Policy
PAGE: 1 of 5	**REPLACES POLICY DATED: 04/2/13**
EFFECTIVE DATE: 03/25/19	**ORIGINAL EFFECTIVE DATE: 04/2/13**
REVISED DATE: 02/26/19	**APPROVED DATE: 03/22/19**
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary of IT Operations	

SCOPE

This policy applies to all North Carolina Department of Health and Human Services (DHHS) workforce members including employees, volunteers, trainees, and other persons who conduct performance of work for a covered entity and who perform duties in conjunction with the access and distribution of protected health information (PHI) and personally identifiable information (PII).

DEFINITIONS

Negligent – A accidental or inadvertent violation due to the lack of proper education.

Gross Negligence- A purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations.

Workforce Member - include employees, volunteers, trainees, and other persons whose conduct performance of work for a covered entity is under the direct control of such entity whether they are paid or note paid by the covered entity.

Protected Health Information (PHI) - Any individual identifiable health information, including genetic information and demographic information, collected from an individual that is created or received by a covered entity.

Personally Identifiable Information (PII) - Information which can be used to distinguish or trace an individual's identity alone (name, social security number, biometric records, etc.) or when combined with other personal or identifying information which is linked or linkable to a specific individual.

Sanction – a penalty for not abiding by a law, rule, or standards set. Official permission or approval for an action.

PURPOSE

The NC DHHS has adopted this policy to facilitate compliance with Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), 45 CFR Parts 160 and 164, and the HIPAA Standards for the Protection of Electronic Protected Health Information (Security Standards). This policy must be applied consistently.

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DIVISON: NC DHHS Privacy and Security Office	**POLICY NAME:** Workforce Sanction Violation Policy
PAGE: 2 of 5	**REPLACES POLICY DATED: 04/2/13**
EFFECTIVE DATE: 03/25/19	**ORIGINAL EFFECTIVE DATE: 04/2/13**
REVISED DATE: 02/26/19	**APPROVED DATE: 03/22/19**
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary of IT Operations	

POLICY

NC DHHS is committed to ensuring the confidentiality and integrity of protected health information (PHI). This policy addresses the appropriateness of applying HIPAA sanctions for violations relating to the unauthorized access, use, disclosure, or destruction of PHI and PII. Sanctions will be imposed upon members of the DHHS workforce who fail to comply with NC DHHS breach notification policies and procedures. Violations of this policy may subject an employee to disciplinary action up to and including termination and any potential civil or criminal sanctions under the law.

PROCEDURE

PHI and PII is considered confidential and may not be accessed or disclosed except as authorized per federal and state requirements. DHHS will investigate any violations and will impose disciplinary measures. The following procedures provides level category guidance (Level 1-4) for violations with examples and recommended appropriate actions.

1. The NC DHHS Privacy Official, the workforce member's manager, Human Resources (HR), and/or the Information Security Official (ISO) must investigate several factors before determining a violation level (**See the Privacy and Security Violation Level Grid below**). The following questions must be considered to determine the workforce member violation:

    - ❖ What is the severity of the violation?
        - o How many patients were affected?
        - o What type of PHI or PII information was inappropriately accessed, used, or disclosed?
        - o To what degree was the confidentiality, integrity, and/or availability of PHI or PII information impacted?
    - ❖ Did the inappropriate action cause harm or is it likely to cause harm to a patient or others?
    - ❖ To what degree was the facility able to verify the specifics of the violation through audit logs, audit trails, interviews, or other investigative factors?

2. In addition to the nature of the violation, the following questions must be considered to determine the severity of the disciplinary action:

DIVISON: NC DHHS Privacy and Security Office	**POLICY NAME:** Workforce Sanction Violation Policy
PAGE: 3 of 5	**REPLACES POLICY DATED: 04/2/13**
EFFECTIVE DATE: 03/25/19	**ORIGINAL EFFECTIVE DATE: 04/2/13**
REVISED DATE: 02/26/19	**APPROVED DATE: 03/22/19**
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary of IT Operations	

- ❖ Has the workforce member been disciplined for violations of privacy and security policy and procedure standards in the past?
- ❖ Has the workforce member completed HIPAA/HITECH training in the last 12 months?
- ❖ How long has the workforce member been employed?
- ❖ Does the workforce member have any other written warnings for other violations in his or her HR file?

3. As the NC DHHS Privacy Official and/or ISO becomes aware of a potential violation and depending upon the severity of the issue, the DHHS Privacy Official and/or ISO may consult with the Privacy and Security Office (PSO).

4. Law enforcement should be contacted for violations that result in the stealing of PHI or PII to commit identity theft and other violations depending on the severity of the violation.

5. Depending on the severity of the issue, the workforce member may be suspended during the investigation of the potential violation in accordance with other human resources policies and procedures. In addition, privileges to mobile devices or laptops may be suspended or revoked depending on the specific issue that has occurred.

6. All documentation pursuant to this policy must be maintained/retained for six (6) years per federal requirements.

7. Any retaliation attempt for reporting a privacy breach or security violation, will be considered a violation of this policy that may result in disciplinary action up to termination of employment or termination of contract with NC DHHS.

Exceptions

Sanctions will not be applied to disclosures by workforce members who are acting in the capacity of a whistleblower or who is a victim of a crime.

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DIVISON: NC DHHS Privacy and Security Office	**POLICY NAME:** Workforce Sanction Violation Policy
PAGE: 4 of 5	**REPLACES POLICY DATED: 04/2/13**
EFFECTIVE DATE: 03/25/19	**ORIGINAL EFFECTIVE DATE: 04/2/13**
REVISED DATE: 02/26/19	**APPROVED DATE: 03/22/19**
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary of IT Operations	

Minimum Recommended Privacy and Security Violation Level Grid

Note: The recommended corrective actions and examples are not intended to capture every situation involving privacy and information security violations. A complete risk assessment and investigation must be performed to determine the most appropriate sanction dependent upon the severity and frequency of the violation(s). Violations may also carry federal civil and/or criminal penalties, and state criminal penalties.

Level Category	**Minimum Recommended Range of Actions for <u>Negligent</u> Violations** *Accidental/inadvertent and/or due to lack of proper education or an unacceptable number of previous violations.*	**Minimum Recommended Range of Actions for <u>Gross Negligence</u> Violations** *Purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations. Proper education previously provided.*
Level 1: Accidental or Inadvertent Violations An unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error accidentally. **<u>Examples:</u>** Directing PHI via mail, e-mail, or fax to a wrong party or incorrectly identifying a patient record.	• Retraining and re-evaluation • Written counseling with discussion of policy and requirements.	• Retraining and re-evaluation • Written counseling with discussion of policy and requirements. *To* • Termination of employment
Level 2: Failure to Follow Established Privacy and Security Policies and Procedures A violation due to poor job performance or lack of performance improvement. **<u>Examples:</u>** Release of PHI without proper patient authorization, failure to report privacy and security violations, improper disposal of PHI, failure to properly sign off from or lock computer when leaving a work station, failure to properly safeguard password, failure to safeguard portable device from loss or theft, or transmission of PHI using an unsecured method.	• Retraining and re-evaluation • Written counselling with discussion of policy and requirements.	• Retraining and re-evaluation • Written counseling with discussion of policy and requirements. *To* • Termination of employment
Level 3: Deliberate or Purposeful Violations Without Harmful Intent An intentional violation due to curiosity or desire to gain information, for personal use. **<u>Examples:</u>** Accessing the information of high-profile people or celebrities or accessing PHI without a legitimate need to know.		• Retraining and re-evaluation • Final written counseling with discussion of policy and requirements. *To* • Termination of employment
Level 4: Willful and Malicious Violations with Harmful Intent An intentional violation causing patient or organizational harm. **<u>Examples:</u>** Disclosing PHI to an unauthorized individual or entity for illegal purposes (i.e., identity theft) or posting PHI to social media websites.		• Retraining and re-evaluation • Final written counseling with discussion of policy and requirements. *To* • Termination of employment

NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DIVISON: NC DHHS Privacy and Security Office	**POLICY NAME:** Workforce Sanction Violation Policy
PAGE: 5 of 5	**REPLACES POLICY DATED: 04/2/13**
EFFECTIVE DATE: 03/25/19	**ORIGINAL EFFECTIVE DATE: 04/2/13**
REVISED DATE: 02/26/19	**APPROVED DATE: 03/22/19**
APPROVED BY: Pyreddy Reddy, CISO; Sam Gibbs, Deputy Secretary of IT Operations	

REFERENCES

Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164

American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D

WORKFORCE SANCTION VIOLATION POLICY/ACKNOWLEDGEMENT OF RECEIPT

I, the undersigned, hereby acknowledge receipt of a copy of the HIPAA Violation Sanction Policy for DHHS.

Dated this _____ day of _____, 20 ____.

_____ _____

Employee Signature Organization

cc: HR Personnel File